WHAT IS CLAIMED IS:

1   1.   A security device comprising:

2   a memory device comprising:

3   a first memory portion configured to store a

4   device ID; and

5   a second memory portion configured to store

6   a device secret;

7   a processor connected to the memory device, the

8   processor configured to read the stored device ID from

9   the first memory portion and the stored device secret

10   from   the   second   memory   portion   and   perform   a

11   nonreversible computation using the stored device ID,

12   the stored device secret, and a challenge as seeds; and

13   a   communication   circuit   connected   to   the

14   processor, the communication circuit configured to

15   receive   the   challenge   from   a   host   device   and   to

16   communicate a result of the nonreversible computation

17   performed by the processor.

25

1   2.   The security device of claim 1, wherein the memory

2   device further comprises:

3   a third memory portion configured to store a

4   service provider data item;

5   wherein the stored service provider data item is

6   also used to seed the nonreversible computation.

1   3.   The security device of claim 2, wherein the memory

2   device further comprises:

3   a fourth memory portion configured to store a

4   counter value that is incremented responsive to the

5   service provider data item being changed;

6   wherein the stored counter value is also used to

7   seed the nonreversible computation.

1   4.   The security device of claim 1, wherein the first

2   memory portion comprises a nonvolatile and unalterable

3   memory device.

1   5.   The security device of claim 4, wherein the second

2   memory portion comprises an unalterable memory portion.

1   6.   The security device of claim 1, wherein the

2   communication circuit operates according to a one-wire

3   protocol.

1   7.   The security device of claim 1, wherein the

2   security device is incorporated into a smart card.

1   8.   The security device of claim 1, wherein the

2   security device is attached to a printer cartridge.

1   9.   The security device of claim 1, wherein the

2   security device is incorporated into a host device.

1   10.   The security device of claim 1, wherein the

2   nonreversible computation is a SHA-1 computation.

1   11.   The security device of claim 10, wherein the

2   processor is configured to perform the SHA-1

3   computation serially.

1   12.   The security device of claim 10, wherein the

2   processor is configured to perform the SHA-1

3   computation in parallel.

27

1   13. A method of device authentication comprising the

2   steps of:

3   receiving a challenge from a device;

4   generating a nonreversible computation result; and

5   outputting a response to the challenge, wherein

6   the outputted response includes the nonreversible

7   computation result;

8   wherein the nonreversible computation result is

9   computed by seeding an algorithm with the received

10   challenge, a device secret, and a unique device

11   identifier.

1   14. The method of claim 13, further comprising the

2   steps of:

3   generating a challenge;

4   transmitting the challenge to the device;

5   receiving a response from the device, the response

6   including the result of the nonreversible computation,

7   which is seeded with at least the challenge; and

8   authenticating the response from the device.

28

1   15. The method of claim 13, wherein the step of

2   receiving comprises the step of:

3   receiving a challenge from a remote security

4   device.

1   16. The method of claim 13, further comprising the

2   steps of:

3   receiving the outputted response at the device;

4   and

5   authenticating the received response.

1   17. The method of claim 15, further comprising the

2   step of:

3   enabling an electronic device responsive to a

4   positive authentication of the received response.

1   18. The method of claim 15, further comprising the

2   step of:

3   disabling an electronic device responsive to a

4   failure to authenticate the received response.

29

1   19. A system for device authentication, the system

2   comprising:

3   a coprocessor security device configured to store

4   a service provider data item and a device secret; and

5   a host device connected to the coprocessor

6   security device, the host device configured to

7   communicate with the coprocessor security device and a

8   roaming security device;

9   wherein the roaming security device can be

10   authenticated to thereby enable the host device.

1   20. The system of claim 19, further comprising:

2   a printer, wherein the coprocessor security device

3   is attached to the printer.

1   21. The system of claim 19, further comprising a means

2   for attaching the roaming security device to a printer

3   cartridge.

1   22. The system of claim 19, further comprising:

2   a means for attaching the roaming security device to a

3   printer.

30

1   23. The system of claim 20, wherein the printer

2   cartridge is disabled responsive to the roaming

3   security device being removed from the printer

4   cartridge.

1   24. A method of device authentication, the method

2   comprising the steps of:

3   receiving, at a roaming device, a challenge from

4   a host device;

5   generating, at the roaming device, a nonreversible

6   computation result, wherein the nonreversible

7   computation result is computed by seeding a

8   nonreversible algorithm with at least the challenge and

9   a device secret; and

10   outputting to the host device a response to the

11   challenge, wherein the outputted response includes the

12   nonreversible computation result.

31

1 25. The method of claim 23, further comprising the
2 steps of:
3   generating a challenge at the roaming device;
4   transmitting the challenge from the roaming device
5 to the host device;
6   receiving a response from the host device, the
7 response including the result of the nonreversible
8 algorithm seeded with at least the challenge; and
9   authenticating, at the roaming device, the
10 response from the host device.

1 26. The method of claim 23, further comprising the
2 steps of:
3   receiving the outputted response at the host
4 device; and
5   authenticating the received response at the host
6 device.

1 27. The method of claim 24, further comprising the
2 step of:
3   enabling an electronic device responsive to a
4 positive authentication of the received response.

32

1   28.   The method of claim 24, further comprising the

2   step of:

3   disabling an electronic device responsive to a

4   failure to authenticate the received response.

1   29.   The method of claim 24, wherein the nonreversible

2   computation result is computed by further seeding the

3   nonreversible algorithm with a unique device

4   identifier.

1   30.   A security device comprising:

2   a memory device comprising a first memory portion

3   configured to store a device secret;

4   a processor connected to the memory device, the

5   processor configured to read the stored device secret

6   from the first memory portion and to perform a hash

7   computation using at least the stored device secret and

8   a challenge as seeds; and

9   a communication circuit connected to the

10   processor, the communication circuit configured to

11   receive the challenge from a host device and to

12   communicate a result of the hash computation performed

13   by the processor.

33

1   31. The security device of claim 30, wherein the

2   memory device is configured to store a partial secret.

1   32. The security device of claim 31, wherein the

2   processor is configured to compute the device secret

3   using the partial secret.

1   33. The security device of claim 30, wherein the

2   memory device further comprises:

3   a second memory portion configured to store a

4   printed page count; and

5   a third memory portion configured to store a

6   maximum page count;

7   wherein the processor is configured to generate a

8   signal responsive to the stored printed page count

9   being equal to or exceeding the stored maximum page

10   count.